AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Ryan S. Burke, depose and state as follows:

AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been so employed since October 2012. I am currently assigned to the FBI's New Hampshire Major Offender Task Force ("NHMOTF") where I am tasked with investigating violent criminals, gang members, and significant drug traffickers throughout the state. As part of the NHMOTF, I work alongside law enforcement officers from various local, state, and federal agencies throughout the state of New Hampshire. I am a "federal law enforcement officer" within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

2. Throughout my career, I have led and/or been involved with investigations of drug distribution, violent crimes, and other offenses. My investigations have included the use of the following investigative techniques: physical surveillance; handling of cooperating sources and witnesses; exploitation of cellular, social media, and Internet Protocol ("IP") based communications data; execution of search and seizure warrants; wire, electronic, and oral wiretaps; and the execution of arrest warrants. Based on my training, experience, and information provided to me by other law enforcement officers, I am familiar with the modus operandi used by individuals engaged in the commission of various criminal offenses, such as those related to acts of violence, firearms, and controlled substances.

PURPOSE OF AFFIDAVIT

3. I submit this affidavit in support of an application for a warrant authorizing the seizure, search, and digital extraction of one cellular phone – described in Attachment A – for the information described in Attachment B. The cellular phone (hereafter, the "Target Device") is

currently in the possession of Destinee Fitz within the District of New Hampshire. It is described as follows:

a. Apple iPhone assigned phone number 603-785-8458 and/or bearing International Mobile Equipment Identity ("IMEI") 356370160354129 which belongs to Destinee Fitz.

4. Based on the information contained herein, there is probable cause to believe the Target Device contains evidence of violations of 21 U.S.C. §§ 841 & 846 (Distribution of Controlled Substances, Conspiracy to Distribute Controlled Substances) committed by Destinee Fitz, Shannon Pellot-Sosa, and others.

5. The information set forth in this affidavit is based on my personal participation in this investigation, as well as my training and experience, and information received from other law enforcement officers. I have not set forth every detail I or other law enforcement officers know about this investigation but have set forth facts that I believe are sufficient to evaluate probable cause of the issuance of the requested warrants.

PROBABLE CAUSE

6. On March 21, 2022, law enforcement directed a Cooperating Witness ("CW-1")[1] to call the Target Device in order to arrange the purchase of two ounces of methamphetamine from Fitz. CW-1 had previously informed law enforcement that Fitz acknowledged an individual named "Craig" was Fitz's methamphetamine supplier. During the recorded call to the Target Device, CW-1 asked Fitz to call "Craig" and inform him that CW-1 needed two ounces. Fitz concurred.

[1] CW-1 has been cooperating with law enforcement since approximately September 2021. During that time, law enforcement believes CW-1 has been truthful and reliable. CW-1 has provided information related to criminal activity which has been corroborated by law enforcement and other witnesses. CW-1 has convictions for the following offenses: Criminal Threatening [M] (NH RSA 631:4); Theft by Unauthorized Taking [M] (NH RSA 637:3); and Possession of Controlled Drug [M] (NH RSA 637:3).

7. On March 24, 2022, Fitz informed CW-1 via iMessage from the Target Device that, "I just talked to him. He's in Manch n I can get u the 2." Fitz also stated the two ounces would cost $1,250.

8. On March 25, 2022, CW-1 was searched by law enforcement and confirmed not to be in possession of controlled substances. CW-1 was subsequently provided a concealed audio/video recorder and followed by law enforcement to Fitz's residence – 389 Front Street, Manchester, New Hampshire ("Residence 1"). Upon arrival, Fitz was observed exiting the residence, entering CW-1's vehicle, and exchanging approximately 55 grams of a substance which field-tested positive for methamphetamine for $1,250. Based upon the recorded phone call and iMessages, I believe Fitz utilized the Target Device to facilitate the acquisition of methamphetamine from her supplier and to facilitate the distribution of methamphetamine to CW-1.

9. On April 4, 2022, law enforcement directed CW-1 to communicate via iMessage with the Target Device in order to arrange the purchase of two ounces of methamphetamine from Fitz. In response, CW-1 received an iMessage from the Target Device wherein Fitz stated, "The two zips[2] is gonna be 1450." When questioned about the increase in price, Fitz replied via iMessage from the Target Device stating, "Different connect[3], better shit." On the following day, Fitz adjusted the price to $1,200 after negotiations with CW-1 via the Target Device.

10. On April 5, 2022, CW-1 was searched by law enforcement and confirmed not to be in possession of controlled substances. CW-1 was subsequently provided a concealed audio/video recorder and followed by law enforcement to Residence 1. Upon arrival, CW-1 called the Target

[2] Based on my training and experience, I know "zip" is a term commonly used by drug traffickers to refer to an ounce of controlled substances.
[3] Based on my training and experience, I know "connect" is a term commonly used by drug traffickers to refer to a source of supply.

Device and Fitz instructed CW-1 to meet at a nearby convenience store. CW-1 was followed by law enforcement to the store.

11. Soon after, Fitz exited Residence 1 and walked to 461 Front Street, Manchester, New Hampshire ("Residence 2") where law enforcement observed her meeting with Pellot-Sosa. Pellot-Sosa then drove Fitz to meet with CW-1 at the store. During their meeting, Fitz provided CW-1 with approximately 53.3 grams of a substance which field-tested positive for methamphetamine in exchange for $1,200. Based upon the aforementioned, I believe Fitz utilized the Target Device to facilitate the acquisition of methamphetamine from Pellot-Sosa and to facilitate the distribution of methamphetamine to CW-1.

12. On April 13, 2022, law enforcement directed CW-1 to communicate via iMessage with the Target Device in order to arrange the purchase of two ounces of methamphetamine from Fitz. Upon agreement, Fitz used the Target Device to send the following iMessage, "So for the zips tomorrow can you try to get the money and get to me by 11 AM because my people have to takeoff to go to New York…" On the following day, CW-1 sent iMessages to the Target Device to modify the order of methamphetamine from two ounces to one ounce.

13. On April 14, 2022, CW-1 was searched by law enforcement and confirmed not to be in possession of controlled substances. CW-1 was subsequently provided a concealed audio recorder and followed by law enforcement to Residence 1. Upon arrival, CW-1 met with Fitz inside Residence 1 and provided her with $600. Fitz then directed CW-1 to wait down the street while Fitz went to obtain the methamphetamine from her supplier. They both then departed from Residence 1.

14. Upon departure from Residence 1, Fitz rode her scooter directly to Residence 2 and entered the front door. After some time, Fitz exited Residence 2 and met with CW-1 across the

street. During their meeting, Fitz provided CW-1 with approximately 25 grams of a substance which field-tested positive for methamphetamine in exchange for $600. Based upon the aforementioned, I believe Fitz utilized the Target Device to facilitate the acquisition of methamphetamine from Pellot-Sosa and to facilitate the distribution of methamphetamine to CW-1.

15. Following the three controlled purchases of methamphetamine described above, law enforcement utilized a subpoena to compel the production of cellular records from T-Mobile related to phone number 603-785-8458. The cellular records confirmed the phone number was associated with a device bearing IMEI 356370160354129 for the entirety of the communications surrounding the controlled purchases. Thus, I know the Target Device was utilized by Fitz to facilitate the controlled purchases described above.

USE OF CELLULAR PHONES TO FACILITATE CRIMINAL ACTIVITY

16. Based upon training, knowledge, and experience as well as from information obtained from other law enforcement officers, I know that it is common practice for individuals engaged in criminal activity to routinely utilize cellular phones, text messaging apps, social media, and coded communications to interact with and do business with co-conspirators. Further, I know that individuals engaged in criminal activity often use cellular phones to plan and facilitate criminal activity.

17. Therefore, I know that evidence of the crimes listed above can be found in cellular phones similar to the Target Device. Such evidence includes, but is not limited to:

a. Names, addresses, telephone numbers, usernames, and email addresses of co-conspirators;

b. Messages/emails sent to or received from co-conspirators or other entities necessary for conducting illegal activity such as arranging travel and transportation;

c. Photographs/videos of themselves and co-conspirators;

d. Photographs/videos of contraband and proceeds of illegal activity;

e. Records of social media and app usage in furtherance of illegal activity;

f. Records of internet activity in furtherance of illegal activity;

g. Calendar entries and to-do lists; and

h. Financial information and bank accounts used in furtherance of illegal activity.

TECHNICAL INFORMATION

18. Based upon my training, knowledge, and experience, I know that cellular telephones such as the Target Device are capable of storing information including, but not limited to, text and audio communications, call history, contact information, calendar entries, downloads, applications, videos, photographs, and electronic documentation in the cellular telephone's memory. In addition, I know that a forensic examination of a cellular telephone and these other devices can result in the retrieval of such data which has been stored on them, even after the passage of time, because files that have been hidden or deleted can still be recovered.

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless

telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can

also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and

utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. I know that many smartphones like the Target Device (which are included in Attachment B's definition of "computer hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. Based on my training, experience, and information provided to me by other law

enforcement personnel, I am aware that individuals commonly store records of the type described in Attachment B in mobile phones, computer hardware, computer software, and storage media.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Target Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Target Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution*. This warrant seeks permission to seize a device currently in the possession of Fitz. If granted, law enforcement will execute the seizure of the device during daytime hours in a place where law enforcement is lawfully present. This warrant also seeks permission to examine the device. Consequently, I submit there is reasonable cause for the Court to authorize the examination to take place at any time in the day or night.

FINGERPRINT AND FACIAL RECOGNITION UNLOCKING

25. Based on my training and experience, I believe it is likely that the Target Device can be unlocked via the use of a fingerprint or facial recognition in lieu of a numeric or alphanumeric password. In my training and experience, users of Apple devices that offer Touch ID or facial recognition often enable it because it is a more convenient way to unlock the device than by entering a passcode. It is also a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

26. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID or facial recognition enabled, and a passcode must be used instead, such as: (1) when a certain amount of time has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID or facial recognition recently and the passcode or password has not been entered in the last few days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID or facial recognition exists only for a short time.

27. The passcode that would unlock the Target Device is not known to law enforcement. Thus, it may be necessary to press the fingers of the user of the device to the device's Touch ID sensor or put the device's camera in front of the user's face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock devices with the use of the fingerprints or facial profile of the user is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

SEALING REQUEST

28. I submit that there is reasonable cause to seal all documents related to this warrant because I believe premature disclosure may cause adverse results, including endangering the safety of cooperating witnesses or law enforcement agents, flight of Fitz, Pellot-Sosa, or others from prosecution, and destruction of evidence.

CONCLUSION

29. Based on the foregoing, I believe the Target Device is utilized by Fitz to facilitate violations of 21 U.S.C. §§ 841 & 846 (Distribution of Controlled Substances, Conspiracy to Distribute Controlled Substances). Consequently, I believe a search and digital extraction of the Target Device will yield evidence of those violations committed by Fitz and others.

/s/ Ryan S. Burke
Ryan S. Burke, Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. P. 41 and affirmed under oath the contents of this affidavit and application.

Date: Apr 29, 2022

Time: 11:12 AM, Apr 29, 2022

Hon. Andrea K. Johnstone
United States Magistrate Judge

ATTACHMENT A

Description of Equipment to Be Searched

The equipment to be searched consists of the following (hereafter, the "Target Device"):

a. Apple iPhone assigned phone number 603-785-8458 and/or bearing International Mobile Equipment Identity ("IMEI") 356370160354129 which belongs to Destinee Fitz.

This warrant authorizes the forensic examination of the Target Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Description of Information or Items to Be Seized

I. All records on the Target Device described in Attachment A, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841 & 846 (Distribution of Controlled Substances, Conspiracy to Distribute Controlled Substances) involving Destinee Fitz and other co-conspirators including but not limited to:

A. Evidence of who used, owned, or controlled the equipment;

B. Evidence of the user's past whereabouts;

C. The identities and aliases of individuals who participated in the violations listed above;

D. Lists of associates and related identifying information;

E. Content associated with the above violations;

F. All bank records, checks, credit card bills, account information, and other financial records;

G. The locations where evidence, fruits, instrumentalities, or other items related to the violations listed above were obtained, is stored, or has been discarded;

H. The methods of communication between individuals engaged in the violations listed above, including the telephone numbers, messaging applications, and social media accounts used by the individuals;

I. The substance of communications regarding the planning, execution, transactions, and/or discussions of the violations listed above;

J. The substance of communications regarding the acquisition or disposal of items involved in the violations listed above;

K. The substance of communications regarding controlled substances, money, vehicles, communications devices, or other items acquired during or for activity that would result in the violations listed above;

L. Photographs of items or information related to the violations listed above;

M. The relationship between the users of the equipment and other co-conspirators;

N. The identity, location, and travel of users of the Target Device and any co-

conspirators, as well as any co-conspirators' acts taken in furtherance of the violations listed above;

O. Evidence of malicious computer software that would allow others to control the equipment, software, or storage media, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

P. Evidence of the attachment of other hardware or storage media;

Q. Evidence of counter-forensic programs and associated data that are designed to eliminate data;

R. Passwords, encryption keys, and other access devices that may be necessary to access the equipment;

S. Records relating to accounts held with companies providing Internet access or remote storage of either data or storage media; and

T. Records relating to the ownership, occupancy, or use of the location from which the equipment was obtained by law enforcement investigators.

II. Evidence of user attribution showing who used or owned the Target Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

III. Serial numbers and any electronic identifiers that serve to identify the equipment.

DEFINITIONS

For the purpose of this warrant:

A. "Equipment" means any hardware, software, storage media, and data.

B. "Hardware" means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Return of Seized Equipment

If, after inspecting seized equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity and accuracy (but not necessarily relevance or admissibility) for evidentiary purposes.

If equipment cannot be returned, agents will make available to the equipment's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying

information of victims; or the fruits or instrumentalities of crime.

Fingerprint and Facial Recognition Unlocking

Law enforcement personnel are authorized to press the fingers (including thumbs) of Destinee Fitz to the fingerprint sensor of the Target Device and/or hold the Target Device in front of the face of Destinee Fitz for the purpose of attempting to unlock the Target Device in order to search the contents as authorized by this warrant.